REPORT DOCUMENTATION PAGE	Form Approved OMB NO. 0704-0188

Public Reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comment regarding this burden estimates or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington Headquarters Services, Directorate for information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188,) Washington, DC 20503.

1. AGENCY USE ONLY (Leave Blank)	2. REPORT DATE 01-December 06	3. REPORT TYPE AND DATES COVERED Final 01 May 01 - 31 Aug 06

4. TITLE AND SUBTITLE

Advanced Tool Integration for Embedded System Assurances

5. FUNDING NUMBERS

DAAD19-01-1-0473

6. AUTHOR(S)

Dr. Insup Lee

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)

Trustees of the University of Pennsylvania,
3451 Walnut Street

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES)

U. S. Army Research Office
P.O. Box 12211
Research Triangle Park, NC 27709-2211

10. SPONSORING / MONITORING AGENCY REPORT NUMBER

42361.11-CI-CIP

11. SUPPLEMENTARY NOTES

The views, opinions and/or findings contained in this report are those of the author(s) and should not be construed as an official Department of the Army position, policy or decision, unless so designated by other documentation.

12 a. DISTRIBUTION / AVAILABILITY STATEMENT

Approved for public release; distribution unlimited.

12 b. DISTRIBUTION CODE

13. ABSTRACT (Maximum 200 words)

The goal of the project is to develop a principled, model-based, and tool-supported approach to design and implementation of embedded systems with high assurance of reliability. Embedded systems consist of a collection of components that interact with each other and with their environment through sensors and actuators. Embedded systems are characterized by the nature of resource limitations and constraints that need to be considered during development and deployment. Embedded systems have been developed traditionally in an ad-hoc manner by practicing engineers and programmers.

We have developed a framework for the integration of a suite of methods and tools for the specification, analysis, development, testing, prototyping, simulation and monitoring of embedded software. The framework is called HASTEN (High Assurance Systems Tools andEnvironments) and is based on systems that support formal specification and verification, test generation from specifications, prototyping and simulation, and run-time monitoring and checking. The technical approach uses mathematical foundations of hybrid systems theory that combines tools from control theory (optimal control, dynamical systems) and software engineering (concurrency, compositionality, model checking).

14. SUBJECT TERMS

15. NUMBER OF PAGES

16. PRICE CODE

17. SECURITY CLASSIFICATION OR REPORT UNCLASSIFIED	18. SECURITY CLASSIFICATION ON THIS PAGE UNCLASSIFIED	19. SECURITY CLASSIFICATION OF ABSTRACT UNCLASSIFIED	20. LIMITATION OF ABSTRACT UL

Enclosure 1

Advanced Tool Integration for Embedded System Assurance

ARO URI Closeout Report

1 Administrative

MURI grant number: DAAD-19-01-1-0473.

Project title: Advanced Tool Integration for Embedded System Assurance.

Duration of the MURI grant: 6/1/01–4/30/06.

Program Manager:

Dr. David Hislop, Army Research Office

Principal Investigator:

Prof. Insup Lee, University of Pennsylvania

Institution:

University of Pennsylvania
3451 Walnut Street Room P221
Philadelphia, PA 19104

MURI Team:

University of Pennsylvania	Prof. Insup Lee
	Prof. Rajeev Alur
	Prof. Sampath Kannan
	Dr. Oleg Sokolsky
University of Illinois,	Prof. Carl Gunter
Urbana-Champaign	Dr. Elsa Gunter
University of Michigan	Prof. Kang Shin

Most recent program review: 5^{th} Annual Review and Workshop of the High-Confidence Embedded Systems program, May 10-11, 2005. Government participants included Dr. David Hislop, Army Research Office, Mr. Bruce Lewis, Army Missile Command, Mr. Paul Jones, U.S. Food and Drug Administration.

2 Program Objective

The goal of the project is to develop a principled, model-based, and tool-supported approach to design and implementation of digital software interacting with physical environment with high assurance of reliability. The technical approach uses mathematical foundations of hybrid systems theory that combines tools from control theory (optimal control, dynamical systems) and software engineering (concurrency, compositionality, model checking).

3 Accomplishments

We have developed a framework for the integration of a suite of methods and tools for the specification, analysis, development, testing, prototyping, simulation and monitoring of embedded software. The framework is called HASTEN (High Assurance Systems Tools and Environments) and is based on systems that support formal specification and verification, test generation from specifications, prototyping and simulation, and run-time monitoring and checking.

A software engineering process is centered around the development of two entities, requirements artifacts and system artifacts, and the validation of system artifacts with respect to requirements artifacts. Requirement artifacts, initially constructed informally through the requirements elicitation, are gradually refined into more rigorous representations. System artifacts can range from design documents and specifications, to prototypes and specifications, to executable code. Each of them are developed to satisfy some of the requirements. Techniques such as prototyping, simulation, verification, testing, and monitoring can be used to evaluate that a system artifact meets its requirements during development and deployment of the system. Evaluation results are used as feedback to modify the system artifacts, and sometimes the requirements. Any changes to the system and requirement artifacts, in turn, necessitates a new round of analysis.

Individual techniques that we have developed to support the HASTEN framework include:

End-to-end analysis of embedded systems. AIRES (Automatic Integration of Reusable Embedded Software) is a software toolkit for high-level design and end-to-end analysis of embedded/real-time systems. Application software is modeled as graphs that represent tasks and their interconnections. AIRES then explores allocations of application software to the hardware platform, to help designers make design decisions such as task formation and priority assignment, and perform a schedulability analysis.

Hierarchical modeling and analysis of hybrid systems. We model embedded systems applications using the modeling language CHARON, which combines discrete mode switching represented as hierarchical state machines enriched with continuous behaviors expressed by differential equations.

Code generation from hybrid systems models. We define a series of formal transformations of the original model that gradually evolve into C++ code, preserving the original model semantics.

Model-driven test generation. Test generation based on extended finite state machine (EFSM) models is performed using coverage criteria based on control flow and data flow in the system. In addition, an extension to the CHARON toolset implements a randomized test generation approach, which allows to quickly accumulate substantial coverage of the model in the cases that cannot be analytically processed.

Run-time verification. Monitoring and run-time checking of compliance with requirements relies on automatic generation of checkers from requirements artifacts. Checkers operate on a sequence of events monitored from a running system. Automatically generated instrumentation probes ensure that all information relevant to checking of a given property is performed.

Interface synthesis for software objects. We have developed JIST (Java Interface Synthesis Tool), which is a set of automated tools and techniques to synthesize interfaces to Java modules. Given a Java class file F that offers a set of method calls M, an interface to F is a small set of rules that capture the correct sequences of calls of methods in M. The JIST tool extracts a small interface for a Java class automatically using boolean abstraction of Java byte code, followed by solving games over the boolean model using state-space exploration heuristics (BDDs, SAT solvers, etc.).

Research supported by the project resulted in 22 publications in peer-reviewed jounals, 89 publications in refereed conference proceedings, and one book chapter. One patent application has been filed. The project supported 16 Ph.D. students, 6 M.Sc. students, and one post-doctoral fellow.

4 Suggestions for the Future

Overall, the project led to a number of successful developments that have reached, or are close to reaching, the technology transfer stage. At the same time, a number of hard open problems in the high-confidence embedded systems area remain. While academic research will be able to make further progress towards solving these problems, its full potential will be realized only through team projects that combine academic researcher with domain experts from industry.